04-298

DivXNetworks, Inc.
10350 Science Center Drive
Building 14, Suite 140
San Diego, California 92121
main 858.909.5300
fax 858.909.5301
http://www.divxnetworks.com
http://www.divx.com

ORIGINAL

July 21, 2004

Federal Communications Commission
Office of the Secretary
Attn: Broadcast Flag Certifications
9300 East Hampton Drive,
Capitol Heights, MD 20743

Re: Request for DivX Networks, Inc., (DXN) for Confidential Treatment of Proprietary and Commercially Sensitive Information contained in Exhibit 5 of the attached Submission for Broadcast Flag Certification

Dear Ms. Dortch:

Pursuant to Section 0.459 of the rules of the Federal Communications Commission (the "Commission"), DivXNetworks, Inc. ('DXN"), with this letter, hereby requests confidential treatment of Exhibit 5 of the attached submission on the basis that the information is proprietary and commercially sensitive. This Exhibit is the License Agreement offered by DXN for the implementation of DXN intellectual property into Integrated Circuits (ICs) and Consumer Electronics devices and is not provided to any person outside of a situation in which its confidentiality is ensured (through a non-disclosure agreement or its equivalent). The full License Agreement is submitted for the Commission's determination that DXN offers fair and reasonable economic terms to all DXN licensees. DXN requests that the License Agreement referenced in Exhibit 5 remains confidential in its entirety.

Since the submission of the full License Agreement serves to assist the Commission in its approval of certain DXN technology as a copy protection technology under the Commission's interim procedures, DXN believes that the request for confidential treatment serves the purposes of this proceeding while maintaining DXN's legitimate interests in preserving the confidentiality of the full License Agreement. DXN is amenable to "protective order"-based disclosure to counsel for other participants in this proceeding so long as (i) such disclosure is restricted to such counsel and only for the purposes of this proceeding, (ii) the disclosed information is returned to the Commission or certified as having been destroyed at the conclusion of the proceeding and (iii) violations of the protective order will subject violators to legal penalties. DXN respectfully requests the opportunity to review any proposed protective order for the purpose of providing further comment on such specific document prior to the release of its Confidential Exhibit 5 to any party other than the Commission.

If this request for confidentiality is denied, DXN would respectfully request that Exhibit 5 be returned to DXN pursuant to the Commission's rules.

If you have any questions concerning this request or submission, please do not hesitate to contact me at the telephone number(s) listed below.

Sincerely,

Adrienne Pierre

Adrienne Pierre
Director, Business Development
DivXNetworks, Inc.
858-449-9056 Cell
858-909-5344 DID

encl: 1 Original, 4 copies

cc: Chief, FCC Media Bureau
Attn: Broadcast Flag Certifications
445 12th Street, SW
Washington, DC 20554

MB 04-298

ORIGINAL

DivXNetworks, Inc.
10350 Science Center Drive
Building 14, Suite 140
San Diego, California 92121
main 858.909.5300
fax 858.909.5301

http://www.divxnetworks.com
http://www.divx.com

July 21, 2004

Federal Communications Commission
Office of the Secretary
Attn: Broadcast Flag Certifications
9300 East Hampton Drive,
Capitol Heights, MD 20743

Re: CERTIFICATION OF DIVXNETWORKS, INCORPORATED's DRM TECHNOLOGY FOR USE WITH BROADCAST FLAG FOR DIGITAL BROADCAST CONTENT PROTECTION

Dear Ms. Dortch:

Enclosed please find a Broadcast Flag Certification submission from DivXNetworks, Inc. ("DXN"), filed under Section 73.9008(c) of the Report and Order and Further Notice of Proposed Rulemaking dated November 4, 2003, MB Docket 02-230.

Please do not hesitate to contact me at the telephone number below if you have any questions concerning this submission.

Sincerely,

Adrienne Pierre
Director Business Development
DivXNetworks, Inc.
858-449-9056

encl: 1 Original, 4 copies,

cc: Chief, FCC Media Bureau
Attn: Broadcast Flag Certifications
445 12th Street, SW,
Washington, DC 20554

ORIGINAL

Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of:	)	
Digital Broadcast Content Protection	)	
	)	MB Docket 04-___
Certification of DivXNetworks, Inc.	)	
Digital Rights Management Technology for	)	
Use with Broadcast Flag	)	

CERTIFICATION OF DIVXNETWORKS, INCORPORATED's DRM TECHNOLOGY FOR USE WITH BROADCAST FLAG FOR DIGITAL BROADCAST CONTENT PROTECTION

DivXNetworks, Inc. ("DXN") in response to the Public Notice issued by the Federal Communications Commission ("FCC") on January 23, 2004, and the regulations set forth therein, hereby requests review and consideration to be one of the approved technologies for Digital Content Protection. DXN asserts that its Digital Rights Management technology ("DivX® DRM") found in DivX Certified™ technology products meets the Commission's standards and is appropriate for use in covered digital entertainment devices to give effect to the Broadcast Flag.

Executive Summary

DXN's core offering is the DivX ® video codec, it is among the world's most popular video compression technologies with over 120 million users worldwide. The patent-pending (Exhibit 1) DivX® video technology offers DVD-quality at proven better compression than MPEG-2 files, enabling full length films to easily fit on a CD or be delivered over broadband connections. DivX® video technology powers a range of applications that span the convergence value chain, from a secure IP-based video-on-demand service solution to next-generation consumer electronics products and video software applications available on the worldwide market today.

The DivX® technology includes DivX® DRM and is a required element in the DivX® Certification program. DivX® DRM implemented in a DivX® Certified™ recording CE product will detect the Broadcast Flag, and encrypt the video for a particular consumer. This prevents the unlawful and indiscriminant redistribution of marked video content.

The DivX® Certification program requirements as explained in this submission can easily extend to support the rules of the Broadcast Flag without requiring any modification to the millions of existing DivX® Certified™ CE devices available on the market today. Adding Broadcast Flag protection to DivX® Certified™ recording products will allow DivX® Certified™ playback products to use the content. Only when someone tries to indiscriminately redistribute the video content the playback of the video content will be prevented entirely.

In September 2002, DXN launched the DivX® Certification Program (Exhibit 2), which includes a complete Digital Rights Management (DRM) system, enabling video content to securely move throughout the connected home via the Home Area Network and beyond to the Personal Area Network. The DivX® Certification Program is a complete testing process to ensure high quality video playback and the interoperability of DivX® video files, as well as a stringent validation

mechanism to ensure full DRM implementation on all CE devices that carry the DivX® brand. DXN has reasonable and fair licensing terms (Exhibit 5) as evidenced by the volume of Licensees. To date, DXN has over 100 Licensees producing DivX® Certified™ IC, Reference Design and Branded CE devices (Exhibit 3).

The information in Section 1 explains how DivX® DRM works and how it will be applied to marked content to give effect to the Broadcast Flag.

Table of Contents

1. Introduction and Background

DXN is a technology company that specializes in video compression and video security. In an effort to expand beyond personal computers, DXN created the DivX® Certification program to embed DXN video technology and DivX® DRM security components into Integrated Circuits (ICs), Reference Designs and Branded Consumer Electronics devices (Exhibit 2). This includes both playback products and recording products. All DivX® Certified™ playback products include DivX® DRM, which enables playback of encrypted content. DivX® DRM serves as a proven method for protecting digital video content for playback and recording applications. In 2004, over 20 million DivX® Certified™ DVD players, networked digital media adapters, hand held devices, and personal media players will be shipping on a worldwide basis with DivX® DRM playback technology built in. The existing DivX® DRM capabilities provide an immediate means of implementation of the Broadcast Flag requirements.

Any DivX® Certified™ CE recording product will be able to detect the Broadcast Flag and then encrypt the video for a particular consumer. This prevents the unlawful and indiscriminate redistribution of this video content. Specifically, the video content is tied to a consumer identity, and subsequently can only be played back on a controlled limited set of DivX® Certified™ products registered to that consumer for legal allowable usage rights as per the FCC guidelines. The DivX® Certification program has showed it is economically viable and possible to include security technology in mainstream CE products that provide protection and give playback control to video content owners. DivX® technology as an approved technology for the Broadcast Flag means CE entertainment products can continue to be easy to use.

DivX® DRM and the DivX® Certification program supports all the requirements of the Broadcast flag as defined in the "The Report and Order and Further Notice of Proposed

Rulemaking" dated November 4, 2003, MB Docket 02-230. DivX® DRM and the DivX® Certification program can support the Broadcast Flag today because of the following features of the DivX® DRM:

1. **Solid Encryption** – Video and data is encrypted with AES using 128 bit keys.
2. **Hardware Security** – The DivX® DRM broadcast flag solution is for dedicated and certified consumer electronics products, such as DVD players. It is not for generic PCs, for which it is difficult to ensure security. This keeps sensitive cryptographic information off personal computers and in more secure hardware-based systems.
3. **Offline Playback** – CE Players do not need a network or phone connection to play back protected content. A consumer only needs to register their CE product via a web site, which can be done at a store or at home from their own PC.
4. **User Key Based** – Broadcast Flag marked content is encrypted with a unique user key. If a user key is compromised, it only compromises the content the user has recorded. They cannot decrypt content from other users or wholesale break the DivX® DRM.
5. **Central Registration Control for Models** – If a particular product model is deemed insecure, it can be denied activation from the server.
6. **Multiple Certified Hardware Keys** – User key data is encrypted in the registration process with a Certified Hardware Key. If that particular Certified Hardware Key is compromised there are a cache of other keys to choose from. In the case where all the keys were exhausted and renew ability is necessary, then new firmware can be required which updates the keys.
7. **Ease of Use** – Consumers simply record and use the content seamlessly on the DivX® Certified™ CE players they have registered. Thus, it is simple to play a video in one room and easily move it to another registered player in another room. It is only if the consumer

tries to play the recorded video content outside their registered DivX® Certified™ CE products the video content will not play. A menu screen on the registered player informs the consumer that playback is unauthorized.

8. **Leverages Currently Available CE Products** – DivX® Certified™ CE entertainment devices are available now. The built-in DivX® DRM can be used without modification to support video content recorded with a DivX® Certified™ recorder designed to support Broadcast Flag recording.
9. **Simplicity, Cost, and Balance** – Transforming the Broadcast Flag into uniquely encrypted video for a consumer is a straightforward process. DivX® Certified™ products have proven to be available at extremely competitive prices worldwide. In fact, DivX® Certified™ DVD players with DivX® DRM cost the same as DVD players without any DRM. This gives a concrete example of an end-to-end system for delivering secure content. This is truly meeting the test of balancing interests of consumers, content providers, equipment makers, and the marketplace. This balance is a central tenet of DivX® DRM and the FCC's Broadcast Flag regulation.

2. DivX® DRM Technology Broadcast Flag Solution

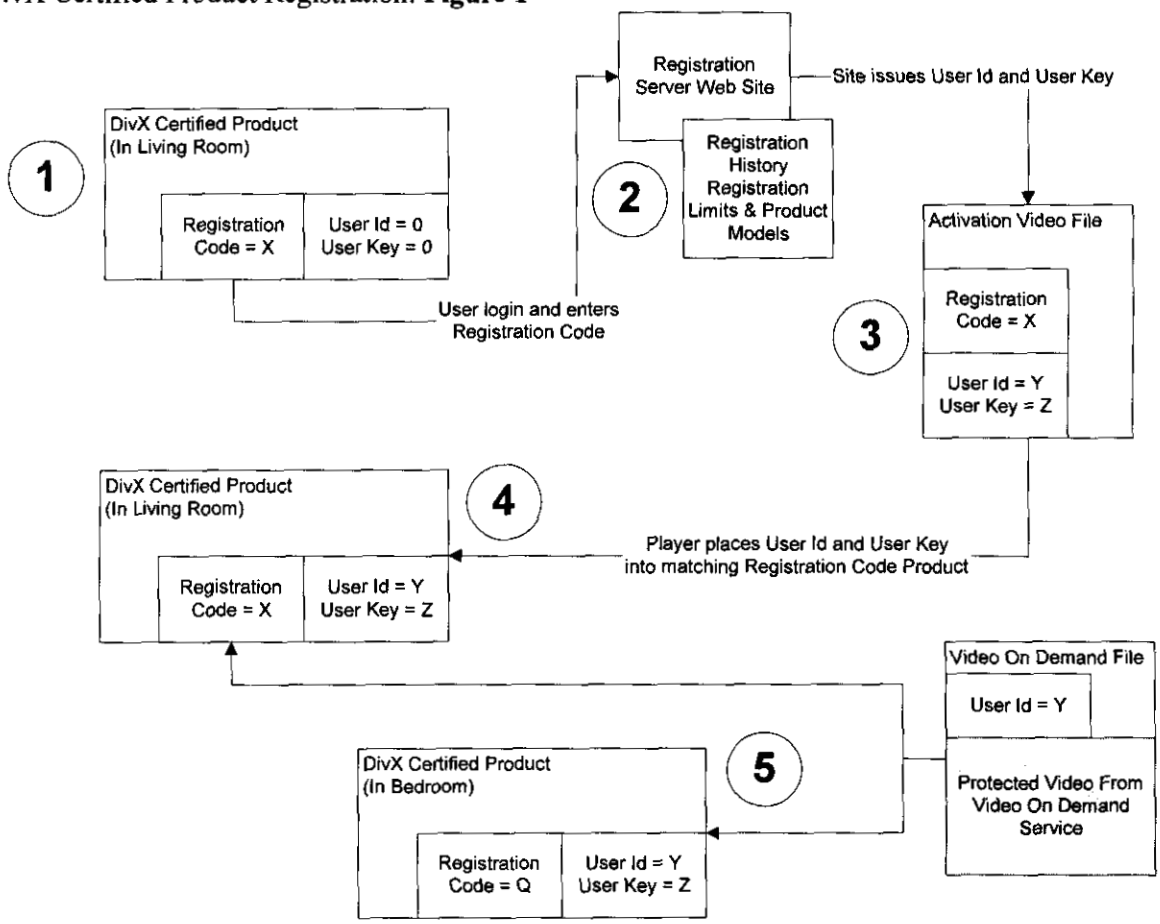
This success of DivX® DRM has depended on the concept of separating the possession of digital content from the ability to play the content. Specifically, DivX® DRM protects (encrypts) digital media content and controls its use. After the digital video content is encrypted, a consumer can only play back the protected file or stream in a device with that consumer's same encrypted key for unlocking the content. This prevents distribution and playback on devices without that consumer's unique key, allowing conditional playback within the home but preventing "indiscriminate distribution". In the Broadcast Flag context, a digital entertainment CE device

supporting DivX® DRM and receiving digital broadcast programming will screen the video content for the presence of the Broadcast Flag. When the DivX® Certified™ CE device detects the Broadcast Flag, it will create and encrypt a DivX® DRM video file which can only be viewed by devices in the home with the consumer's unique key.

When encryption is mentioned, Advanced Encryption Standard (AES) with 128 bit keys is used. Figure 1 illustrates the solution using DivX® DRM technology.

When a consumer purchases a DivX® Certified™ CE entertainment product, registration of the product, with regard to security, is outlined in steps 1-5 in Figure 1 below.

DivX Certified Product Registration: **Figure 1**



1. A new DivX® Certified™ product needs to be registered for a particular user. This happens through a registration code.

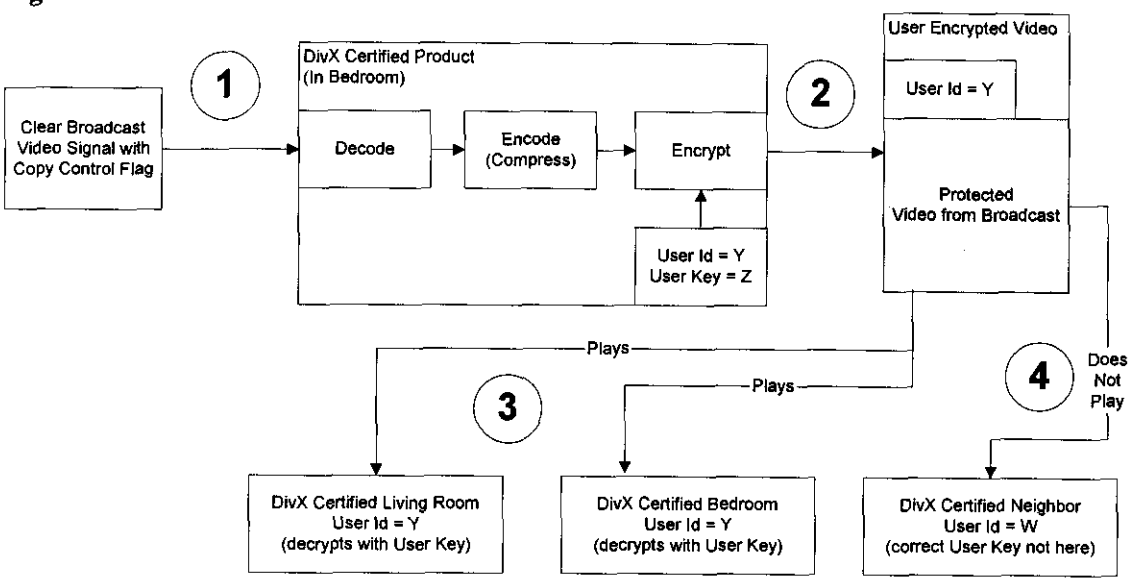
2. The registration code is validated by a network server. This is a crucial control point. The server decides if it is OK to issue an activation file. Only DivX® Certified™ models are allowed to activate, and, if a content provider deems necessary, the consumer will not be allowed to activate the DivX® Certified™ CE device for security reasons.
3. The activation file enables a particular DivX® Certified™ product to be registered to a particular consumer.
4. The consumer plays the activation file and this activation file places the user id and user key into the DivX® Certified™ product.
5. If the consumer wants to register more DivX® Certified™ products, the process is repeated. Note that a different product, such as one in the bedroom as opposed to one in the living room, will have a different registration code. The server defaults to allow only 6 products per 6-month period to be registered to one consumer. This prevents the same user ID and user key to be shared by massive amounts of people. The consumer can now also purchase files from an IP Video On Demand service. As explained in Figure 2, the consumer can also playback video from a flagged broadcast source.

Communications in Figure 1, step 2, are done via Secure Socket Layer version 3 (SSL3) using greater than 80 bit symmetric encryption ciphers, such as DES3 or AES, and signed certificates via RSA. Communication in Figure 1, step 3 and 4, are encrypted via AES with a 128 bit key (a Certified Hardware key) placed into the DivX® Certified™ CE Product. The Certified Hardware key is known only by the registration servers. Additional keys are available in the DivX® Certified™ product to encrypt the data if that key is deemed insecure. In the case of a

complete loss of security of the keys, then new keys can be issued to DivX® Certified™ CE devices for renew ability.

Figure 2, below, in steps 1-4 outlines how the DivX® DRM technology supports Broadcast Flagged video content in DivX® Certified™ CE devices.

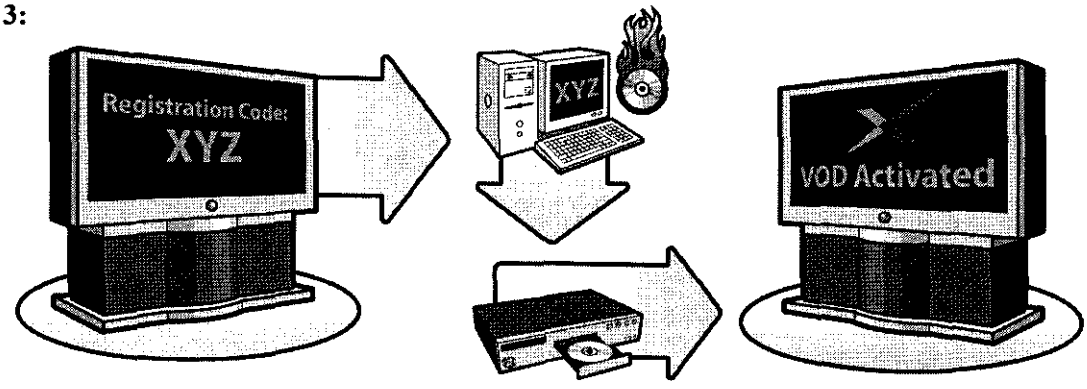
Figure 2



1. A broadcast signal is inputted into a registered product. Once the flag is detected the DivX® DRM technology uses the user key to encrypt the video and labels it for that particular consumer.
2. The output file is now encrypted for that consumer, so it will only play on products that consumer has registered, and registration is limited to a handful (6 in 6 months) of products.
3. The file plays on all the products in the consumer's home.
4. The file does not play on a neighbor's or non DivX® Certified products. Any copy of that video file will not play unless it is for that consumer's DivX® Certified products.

Figure 3 depicts the actual consumer experience during the registration process of a DivX® Certified™ CE device as explained in figures 1 & 2. The consumer simply pulls up the registration code (e.g., XYX)[1] for their DivX® Certified™ CE device, goes to the computer, inputs the code, burns a 15 second activation video file on the PC, then takes the activation CD to their DivX® Certified™ CE device and plays the activation file.

Figure 3:



DivX® DRM firmware distributions to DivX® Certified™ products are encrypted with keys embedded in the hardware for a particular model. Thus, any Certified Hardware keys in the firmware are protected. Also, all distributions of the DivX® technology reference code to CE manufacturers are distributed through Pretty Good Privacy (PGP) with procedures to ensure the correct identity of each CE manufacturer.

3. Additional DivX® Background

The DivX® DRM technology is already a proven method for protecting digital content. As an example, DXN designed and implemented a secure Internet VOD service with DivX® DRM, which has been operating since August 2001 worldwide (Exhibit 4). The DivX® DRM technology

[1] Note: the DivX® registration code in a DivX® Certified™ CE device is an eight (8) character code.

implemented in the service has proven highly reliable against unlawful and indiscriminant redistribution of protected movie content as proven by the availability of more than 15,000 video titles from over 45 content partners as of May 2004, generating millions of dollars in annual revenue.

In addition to the reliability of DivX® DRM, DXN offers reasonable and non-biased licensing terms of use as evidenced by the extensive list of current DivX® Licensees (Exhibit 3), with the goal of creating world-wide acceptance of the DivX® DRM technology. In 2004, IC manufacturers making chipsets for consumer electronic devices are targeted to produce approximately 20 million chipsets with DivX® DRM implemented ensuring the secure playback of video content marked with Broadcast Flag.

Today, over 100 million PC video players are in use, and millions of CE devices from PC peripherals to Portable Media Players and DVD players are enabled with DivX® DRM for secure video playback, not only to the PC, but directly to the TV in consumer's homes around the world.

DivX® DRM is a proven DRM implementation and in place worldwide today by providing a complete solution for the delivery of full screen, DVD-quality video-on-demand (VOD) over Internet Protocol (IP) networks to PCs and multiple convergence CE devices. DXN's flagship product, the Open Video System™ (OVS), is a turnkey, completely integrated backend system allowing content owners to aggregate, promote, distribute, protect, and derive revenue from their content. There are multiple components to the OVS, and perhaps the most important piece is DivX® DRM, which runs seamlessly as a mechanism for protecting video content from indiscriminate redistribution and giving playback control to video content owners.

Exhibit 1

DXN PATENT INFORMATION

US Patent Application No.: 10/731,809
Entitled: File Format for Multiple Track Digital Data
Filed: December 8, 2003,.
Field of Invention: The present invention relates, in general, to data storage and archiving and, more specifically, to file formats for storing multiple tracks or streams of data.

US Patent Application No. 10/693,680
Entitled: "Method and System for Supercompression of Compressed Digital Video"
Filed: October 23, 2003
Field of Invention: The present invention relates to the field of digital video compression. More specifically, the present invention is directed to a method and system for transcoding a compressed video stream into another compressed video stream of lesser bandwidth without loss of video quality by the use of a more efficient entropy coding scheme than was used in the original stream.

US Patent Application No. 10/615,898
Entitled: "Method and System for Securing Compressed Digital Video"
Filed: July 8, 2003
Field of Invention: The present invention relates to the field of the encryption and efficient decryption of video information. More specifically, the present invention is directed to a method and system for generating a protected stream of compressed digital video and for decrypting the protected stream in a bounded-bandwidth fashion

US Patent Application No. *Filed and Pending*
Entitled: "Optimized Secure Media Playback Control"
Filed:
Field of Invention: The present invention relates to managing rights to playback of media content by a player, and more particularly to a system, method and apparatus for managing the rights to playback of media content on a standalone player, such as a player that is currently not connected to a media control server, based on playback control information stored in memory of the player.

Exhibit 2

STEPS TO DIVX® PRODUCT CERTIFICATION

(1) DivX® technology partner signs a license agreement with DivXNetworks.
(2) Depending on the type of license agreement signed, the licensee will receive one or more of the following:

i. DivX® technology from the DivX® Software Developers Kit (SDK). Licensee is responsible to provide a local hardware key to be used for product registration/identification in product key encryption.

ii. DivX® Certification Kit for the type of product being developed. A Kit typically includes –
   a. Certification Requirements
   b. Certification Test Instructions
   c. Certification Test clips
   d. Certification Test Tools
   e. Certification Test Results Form
   f. Certification Branding Guidelines
   g. Official DivX® Video and DivX® Certified Logos

(3) Licensee submits a certification application for either an electronic device or software product to a DivX Certification Center. The web application must be filled out completely. A copy of the completed application must always be included with products shipped to the DivX Certification Center for testing.
http://www.divxnetworks.com/support/hwcertification.php

(4) Licensee is contacted by DXN Technical Support to schedule a Certification Requirements Technical Overview. A meeting may be scheduled at the customer's request to review the certification requirements and certification kit contents with licensee's assigned engineers and/or project manager.

(5) Licensee is contacted by DXN Account Management to schedule a Certification Program Overview. A meeting is scheduled to review the agreement terms, roles and responsibilities of both the licensee and DXN, including production planning and reporting, royalties collection, OEM and retailer relationship management with licensee's project manager and financial and/or executive representative.

(6) Depending on the license agreement signed, DXN will issue a DivX® model identifier to the licensee when the completed application is received.

(7) Licensee implements the DivX® technology using the DivX® SDK or obtains an already DivX® Certified component. Licensee should purchase DivX Certified components.

Products that are not using DivX® Certified components may not be compatible or meet DivX® Certification requirements.

(8) Licensee conducts a dry run of the tests required for the targeted product.

(9) DXN Technical Support or a DivX® approved technology partner will assist to resolve questions that arise during the initial product certification dry run testing.

(10) Licensee delivers to the DivX Certification Center:

i. Copy of the Certification Application
ii. Product to be certified
Engineering sample or final product including power supply and cabling.
iii. Dry run test results
Results of the licensee conducted tests to be used as a baseline for DivX Certification Center testing.
iv. Operating instructions
How to start up and use the device, including how to display the version of firmware used in the device. In some instances, it may be desirable for an engineer to accompany the device. This must be pre-arranged with the DivX® Certification Center.
v. Upgrade instructions
Instructions on how to update the firmware for products that offer this capability.

(11) DivX® Certification Center will perform the initial device function test. If there are any problems with the device, the licensee will be notified and attempts will be made to resolve or reschedule the testing.

(12) DivX® Certification Center will verify that all requirements identified in the Certification Requirements document are met for the type of product submitted. The tests identified in the Test Instructions document will be performed and the results recorded in the Test Results form. The test process is normally completed within one week following receipt of a scheduled product. If the product was not scheduled, the testing may take longer depending on demand. Licensee is encouraged to schedule in advance.

(13) Licensee will be contacted when the certification tests are completed. The licensee is notified with the product test results:

i. PASS indicates the licensee is authorized to use the DivX® Logo for the newly certified product.
ii. RETEST indicates the licensee must resolve the noted failure condition(s) and submit corrections to the DivX® Certification Center.

(14) Licensee must meet all product branding requirements prior to being issued the DivX® Certified Product Certificate. When the licensee successfully passes the DivX® Certified Product requirements, Licensee is responsible to ship 2 production units to DXN for firmware and product branding verification. DXN will keep the product submitted by licensee to enable future certification compatibility testing and technical support.

(15) Licensee will receive a DivX® Certified Product certificate that confirms the brand identification, the model number, reference chip and certified firmware version certified by DXN. Licensee will also be contacted by DXN for permission to publish a press release regarding product certification and provide retailer and/or consumer endorsement on the DivX.com web site.

(16) Licensee is contacted by DXN Account Management periodically to schedule certification program updates. A conference call meeting is scheduled to review any open business or relationship issues, production schedules and timelines, contractual issues or any ODM/OEM and retailer relationship management updates with licensee's project manager and financial and/or executive representative.

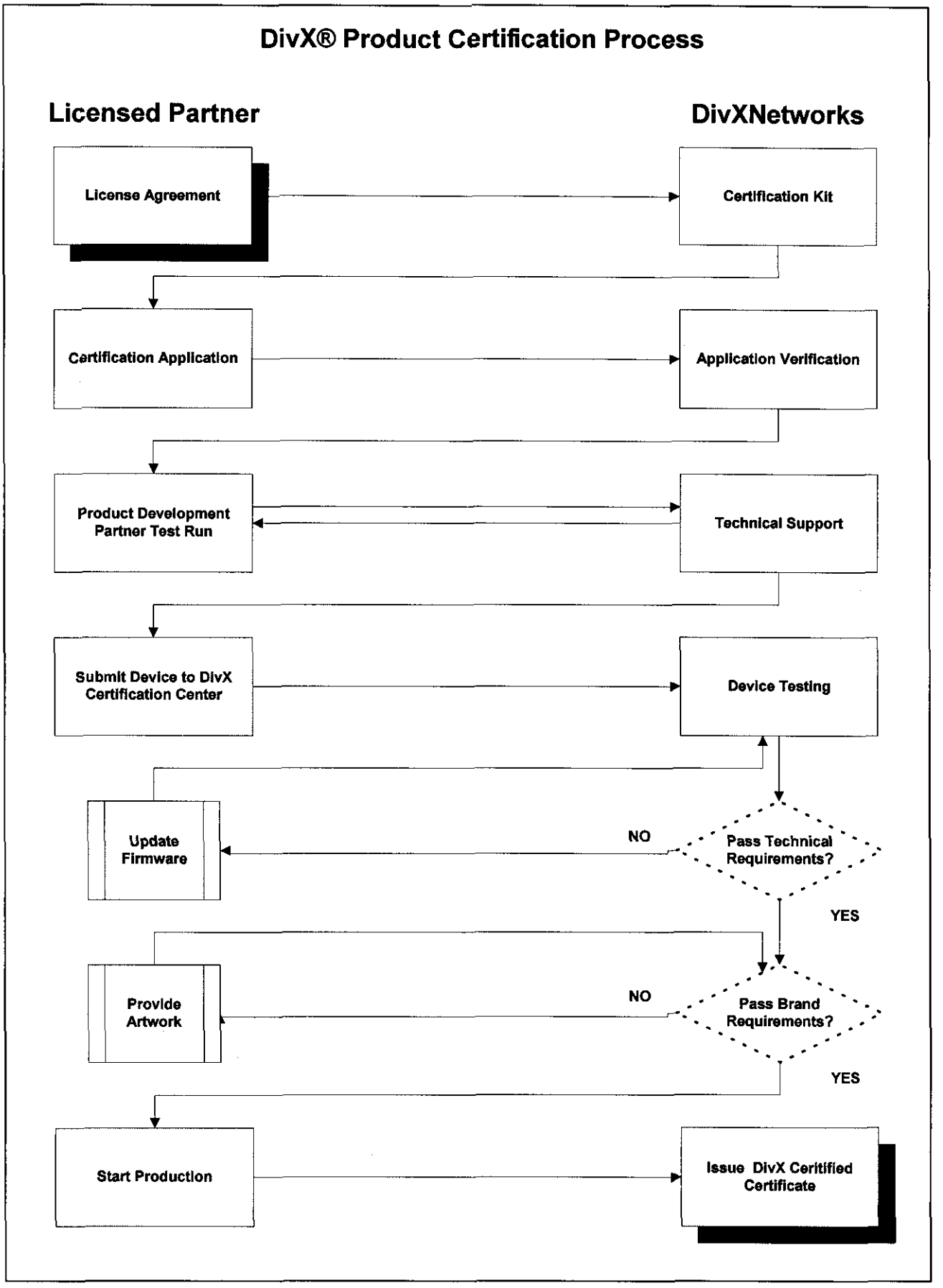

DivX® Product Certification Process
Licensed Partner
DivXNetworks
License Agreement
Certification Kit
Certification Application
Application Verification
Product Development Partner Test Run
Technical Support
Submit Device to DivX Certification Center
Device Testing
Update Firmware
NO
Pass Technical Requirements?
YES
Provide Artwork
NO
Pass Brand Requirements?
YES
Start Production
Issue DivX Certified Certificate

Exhibit 3
DXN LICENSEES

DivX® has partnered with a diverse group of consumer electronics companies working to create a wide selection of DivX® Certified video solutions. From DivX Certified digital cameras and DVD players to portable devices and set-top boxes, DivX video has moved beyond the PC to become a key piece in the convergence puzzle.

DivXNetworks hardware partners include:

- Alarity
- Alba plc
- Alco Electronics Ltd.
- ALi Corporation
- Amlogic
- Amoi Electronics Co., Ltd.
- APS
- Arlink Tech Corporation
- Ascomtec
- AV Industries
- AVAYON Technologies Inc.
- BBK Electronics Corp., Ltd.
- Beautiful Enterprise Co., Ltd
- Bluetek
- ChangZhou XINGQIU Electric Co., Ltd.
- Cheertek Technology
- Cirrus Logic, Inc.
- Cointer Electrónica S.L.
- Cosmic Digital
- Dalian Golden Hualu Digital Tech.
- DAT HK Limited (Daewoo DAT)
- Desay A&V Science and Technology Co., LTD.
- e.Digital
- Digital Square
- Eastern Asia Technology Ltd.
- Elta GmbH
- Emsoft
- Equator
- ESS Technology, Inc.
- Fujitsu Siemens Computers GmbH
- GBM Advanced Technology International Inc.
- Gedelson
- Gericom AG
- Global Create International
- Gowell
- Guillemot (Hercules)
- GVG Digital Technology Holdings (HK) Ltd.
- HandHeld Entertainment (ZVUE)
- HUMAX Co. Ltd.
- IO Data
- Industrial Technology Research Institute (ITRI)
- Ittiam
- Jamo
- Jiangsu Hongtu Technology Co. Ltd.
- JVC
- Kenwood Corporation
- Kinpo
- KiSS Technologies
- L8S Electronik GmbH
- Link Concept Technology Limited
- LG
- LSI Logic
- MagicEyes Digital Co.,Ltd.
- Mecotek International Pte Ltd.
- MediaTek Inc.
- Medion AG
- MIB Partners Limited
- MiCO Electric(Hong Kong) Limited
- Nanjing Wanlida Seeing & Hearing Equipment Co., Ltd.
- Neuston Corporation
- Nintaus Electronics Company Limited
- Nortek S.p.a.
- nReady Netware Limited
- Orient Power Multimedia Ltd.
- Oxford Semiconductor
- The Petters Group (Polaroid)
- Philips Electronics Hong Kong Limited
- Pixa, Inc.
- Plextor
- Rimax
- Roadstar
- RJ Tech
- Samsung
- Sandmartin (Zhong Shan) Electronic Co., Ltd.
- Schneider UK
- Scott DVD GmbH
- Semiconductor Company, Matsushita Electric Industrial Co., Ltd.
- Shenzhen E-boda Technology Co., Ltd.
- Shenzhen GIEC Electronics Co., Ltd.
- Shenzhen KXD Multi-Media Co. Ltd.
- Shenzhen Skywood INFO-TECH INDUSTRIES CO., LTD.
- Shinco Digital Limited
- Siemssen
- Sigma Designs
- Skyworth Multimedia (Shenzhen) Co., Ltd.
- Starlight Video Limited
- Sunplus Technology Co. Ltd.
- Tamul Multimedia, Co., Ltd.
- Thomson (RCA)
- Tonic Digital Products Limited
- Unibrain
- VIA Optical Solution, Inc.
- Vieta Audio S.A.
- Vtrek
- WIS Technologies, Inc.
- Woxter United Corporation, S.L
- Xingqiu
- Yamaha
- Zhenjiang Jiangkui Group Co. Ltd.
- Zhongshan Kenloon Digital Technology Co., Ltd
- Zoran Microelectronics Ltd.